TRIPS Signature Fact Sheet

Problem Description:

For modern industry to migrate to true paperless operation, a trusted means for creating electronic signatures must be available. The electronic signature mechanism must include non-repudiation (validation of both signatures and the original data signed). Currently, electronic signature for "flat files", such as e-mail messages, can be implemented using off-the-shelf technology and industry standards. This is achievable because a flat file, as a single entity, contains all of the data being signed and verified. The electronic signature becomes an inseparable part of that file, much in the same way that a written signature becomes a part of a document. Use of electronic signature technology is growing significantly as more information is exchanged on Internet/Intranets. Most currently acceptable electronic signature systems incorporate Public Key Cryptography Standards (PKCS). PKCS-based electronic signatures are becoming legally valid "signatures" for several federal agencies and state governments.

The need to "sign" information, and provide non-repudiation, is not limited to the information contained in flat files. Much of the electronic data that is subject to review and approval resides in relational databases. The information subject to signature is typically presented to the user as a form or report. Unlike e-mail messages, this data does not reside in one contiguous location as a separate entity, but is made up of source data records crossing multiple tables within a database. There is no known industry-wide solution to sign database entities and still provide non-repudiation of the signature relative to the original data stored in a relational structure.

Current solutions involve: 1) printing computer reports, signing the paper, or 2) filing or digitally scanning documents. Neither one of these solutions provide non-repudiation against the actual source data in the database, which effectively has to be managed and validated separately from the signing process. **A relational database digital signature technology is needed for a truly efficient, validated paperless process. Such technology could be applied to databases containing data with legal significance or national security concerns such as environmental or technical data, financial transactions and work approval databases. This technology would lend well in managing geographically distributed work forces - where signatures are required from individuals in all locations.**

Solution:

Currently, there are no commercial solutions for providing digital signatures for database elements. Because of the industry void, the INEEL is developing technology to create and extend electronic signature industry standard algorithms to database structures.

The new technology provides electronic signatures for database records, ensuring data integrity, user authenticity, and non-repudiation for signatures on specific data base entities. Currently the technology is implemented in INEEL's largest waste inventory processing system, the Transuranic Reporting, Inventory, and Processing System (TRIPS). TRIPS will be used to collect, certify, and electronically sign waste characterization data for 140,000 waste containers that are scheduled to be shipped to Waste Isolation Pilot Plant for disposal. The Department of Energy and the State of New Mexico have accepted this technical solution as a valid in the information review, approval and certification process

The TRIPS application combines PKCS standards with custom application code and database structures designed specifically for the TRIPS application. We propose to convert the TRIPS specific solution to provide a general case technology with implementation toolkits that could be applied to other existing databases.

Benefits of This Solution:

- The digital signature generation process is very efficient. It requires only a few seconds to create and store a signature and even less time to verify a signature.
- Studies have shown that digital signatures are very cost effective, up to 85% savings as compared to paper report based systems.
- Electronic signing of "flat files" is based on industry standards. Applying these same standards to signing a relational database creates an architecture inherently acceptable to industry.
- Public Key Cryptography Standards (PKCS) based electronic signatures are legally valid "signatures" for many government agencies and recognized by the American Bar Association. The electronic approval architecture extends these industry standard algorithms to database structures and produces an electronic signature that ensures data integrity, user authenticity, and non-repudiation of the source data. These criteria are necessary for a legal signature.
- This architecture can be expanded into an implementation that is relatively independent of vendor database, and transferable to different database applications that require non-repudiation.

Market and Commercialization Opportunities:

Although a full market analysis has not been completed, preliminary assessments by Alan Kirsch and Data Access Products managers indicate that this is LMITCO intellectual property with commercial opportunities via software copyrights and/or patents. Databases, electronic approvals, and distributed/networked work forces are very common and represent a large business segment.